communicate with an access device (e.g., access device **102**). In some embodiments, this is accomplished through the use of asymmetric keys.

[0050] For example, a unique asymmetric identity key may be provided for the input device **108** during manufacture or at some later time. The private key portion of this asymmetric key may be stored within a security boundary (e.g., the security module **110**) in the input device **108**. For example, a processor (e.g., a multi-purpose processor or a cryptographic processor) may generate the key within this security boundary and the private portion of the key may never be allowed to appear outside of the security boundary in the clear (i.e., unencrypted). Additional details of a security boundary are provided below.

[0051] The public portion of the key may then be published with a digital certificate. For example, the manufacturer of the input device may publish the public key and the certificate on a publicly accessible server. The certificate may serve to verify that the public key is authentic, that the private key has not been disclosed outside the security boundary and that the input device that holds the private key provides a mechanism to securely receive, use and maintain keys. Thus, the certificate serves to strongly verify the authenticity of any information provided by an input device that has the corresponding private key.

[0052] In some embodiments, the input device and the access device may use the asymmetric key to negotiate one or more other keys that may be used for cryptographic processing. For example, these other keys may be used to encrypt, decrypt, sign, etc., information send between these components. In this way, an authenticated and/or secure channel may be established between the input device and the access device. That is, each component will have one or more keys that enable it to encrypt, decrypt or authenticate information that it sends to or receives from the other component. In this way, sensitive information (e.g., credentials or keys) may be securely sent over a link **118** (e.g., a wireless link such as Bluetooth, etc.) that may not otherwise be secure.

[0053] Referring now to block **204**, keys also may be generated for the security module in the access device during manufacture or at some later time. Thus, a unique asymmetric identity key may be provided for the access device **102**. The private key portion of this asymmetric key may be stored within a security boundary (e.g., the security module **112**) in the access device **102**. The public portion of the key may then be published with a digital certificate that may serve to verify that the public key is authentic, that the private key has not been disclosed outside the security boundary and that the access device that holds the private key provides a mechanism to securely receive, use and maintain keys. Thus, the certificate serves to strongly verify the trustworthiness of the access device. This asymmetric key pair may then be used to establish an authenticated and/or secure channel between the access device and the access server or some other device.

[0054] Referring now to block **206**, once the devices are installed in the field, the devices and the access server may establish secure channels over media that may otherwise be insecure. In some embodiments this may involve performing asymmetric key exchange operations.

[0055] At block **208**, to enable the access server to recognize the credentials assigned to a given user, the credentials are enrolled (e.g., entered into) the access server. This may be accomplished, for example, using a credential enrollment mechanism. Additional details of various credential enrollment mechanisms are discussed below.

[0056] The credential enrollment mechanism provides the credential information to the security module **116** which may then generate one or more keys associated with that credential. These keys may comprise, for example, SSL or IPsec keys/security associations that may enable the user to log onto a security network.

[0057] Referring to block **210**, when a user wishes to access a service via the access device **102**, the user presents his or her credentials to a data input component **122** on the input device **108**. The data input component may comprise a keypad, an RFID reader, a sensor, etc.

[0058] In some embodiments the input device **108** is a biometric sensor. For example, the sensor may comprise a fingerprint reader. Alternatively, the sensor may comprise a retina/iris scanner, an audio input device (e.g., a microphone) for speech recognition, a camera sensor (e.g., a CCD device) for, e.g., facial feature recognition or a DNA typing device. In addition, appropriate processing may be provided on the sensor integrated circuit to facilitate retrieval and analysis of this information.

[0059] In some embodiments credentials may be provided to the input device via a direct path into the security boundary of the input device. For example, credentials may be directly entered into a device located within a security boundary. This may be accomplished, for example, using a keyboard, an RFID reader, a biometric sensor, etc., that is physically attached to a component within the security boundary. Additional details of these types of components are discussed below.

[0060] Referring to block **212**, the input device **108** sends the credentials to the access device **102** via the authenticated and/or secure channel discussed above. For example, a cryptographic processor in the input device may use a key obtained from the negotiation with the access device **102** discussed above to sign and/or encrypt the credentials. Typically, the cryptographic processor signs the credentials using such a key or the private key of the input device.

[0061] Referring to block **214**, the access device **102** processes the credentials, as necessary, and sends the credentials to the access server **106** via the authenticated and/or secure channel **120** discussed above. For example, a cryptographic processor in the access device **102** may use a key obtained from the negotiation with the access server **106** discussed above to encrypt the credentials. Typically, the cryptographic processor signs the credentials using such a key or the private key of the access device **102**.

[0062] At block **216**, cryptographic processor(s) in the access server **106** process the encrypted/signed credentials. Through this cryptographic process, the access server obtains strong authentication that the credentials are from a user that is using a specific access device **102**. Moreover, assurances may be made via the certificate that the input device (e.g., keyboard, sensor, RFID components, etc.) through which a user inputs credentials is proximate to that access device.

[0063] The access server **106** then checks the credential database to verify that the credentials are associated with an